

What is claimed is:

SUB A27

1. A method of enabling a proxy client in a secured network to access a target service on behalf of a user,

5 comprising the steps of:

registering proxy authorization information regarding the user with a trusted security server, the proxy authorization information identifying the proxy client and an extent of proxy authorization;

10 submitting, by the proxy client, a proxy request to the trusted security server requesting access to the target service on behalf of the user;

comparing, by the trusted security server, the proxy request with the proxy authorization information of the user
15 to determine whether to grant the proxy request;

issuing, by the trusted security server, a data structure containing authentication data recognizable by the target service for authenticating the proxy client for accessing the target service on behalf of the user.

20

2. A method as in claim 1, wherein the data structure is a ticket containing a session key for use in a session formed between the proxy client and the target service.

25

3. A method as in claim 1, wherein the ticket is encrypted with a secret key shared by the target service and the trusted security server.

4. A method as in claim 1, wherein the step of comparing determines whether a proxy duration specified by the proxy authorization information has expired.

5

5. A method as in claim 1, wherein the step of submitting the request includes transmitting a ticket for authenticating the proxy client to the trusted security server.

10

6. A computer-readable medium having computer-executable instructions for performing steps:

storing proxy authorization information from a user for authorizing a proxy client to act as a proxy of the user;

15

receiving a proxy request from the proxy client to access a target service on behalf of the user;

determining, based on the proxy authorization information of the user, whether to grant the proxy request;

20

constructing a data structure containing authentication data recognizable by the target service for authenticating the proxy client for accessing the target service on behalf of the user.

25

7. A computer-readable medium as in claim 6, having further computer-executable instructions for performing the step of authenticating the user based on a password of the user before storing the proxy authorization information.

8. A computer-readable medium as in claim 6, wherein the
step of receiving the proxy request includes authenticating
the proxy client based on a ticket issued to the proxy client
5 for communicating with the trusted security server.

9. A computer-readable medium as in claim 6, having
further computer-executable instructions for performing the
step of sending the data structure to the proxy client for
10 presenting to the target service for authentication of the
proxy client.

10. A computer-readable medium as in claim 6, wherein
the data structure is encrypted with a key shared by the
15 target service and the trusted security server.

11. A computer-readable medium having computer-
executable instructions for a client in a secured network
system to perform the steps of:

20 submitting a proxy request to a trusted security server,
the proxy request identifying a user and a target service that
the client intends to access on behalf of the user;

receiving from the trusted security server a session key
encrypted with a shared secret key shared by the client and
25 the trusted security server and a ticket for accessing the
target service;

decrypting the session key with the shared secret key;

constructing an authenticator encrypted with the session key;

presenting the authenticator and the ticket to the target service for authentication of the client for access of the target service on behalf of the user.

12. A computer-readable medium as in claim 11, wherein the step of submitting the proxy request includes sending a ticket issued to the client for authenticating the client to the trusted security server.

13. A computer-readable medium having stored thereon a data structure containing information for proxy authorization, comprising:

15 a first data field containing an identification of a user of a secured network;

a second data field containing an identification of a security principal of the secured network authorized to act as proxy of user;

20 a third data field containing data identifying a duration of proxy authorization;

a fourth data field containing data specifying a restriction on the proxy authorization.

25 14. A computer-readable medium as in claim 13, wherein the data in the third data field specify an expiration date of the proxy authorization.

15. A computer-readable medium as in claim 13, wherein
the data in the fourth data field identify a service of the
secured network that the security principal is permitted to
5 access.

16. A computer-readable medium as in claim 13, wherein
the security principal is a client on the secured network.

10 17. A computer-readable medium as in claim 13, wherein
the security principal is a group on the secured network.